[19]中华人民共和国国家知识产权局

[51]Int.Cl[6]
H04N 7/16
H04N 7/167

[12]发明专利申请公开说明书

[21]申请号 97193565.3

[43]公开日 1999年4月28日

[11]公开号 CN 1215528A

[22]申请日 97.3.21 [21]申请号 97193565.3
[30]优先权
[32]96.4.3 [33]EP [31]96200907.2
[86]国际申请 PCT/EP97/01557 97.3.21
[87]国际公布 WO97/38530 英 97.10.16
[85]进入国家阶段日期 98.9.30
[71]申请人 迪格科公司
地址 荷兰霍夫多普
[72]发明人 西蒙·鲍尔·阿什利·里克斯
安德鲁·格拉斯普尔
多纳德·瓦茨·戴维斯

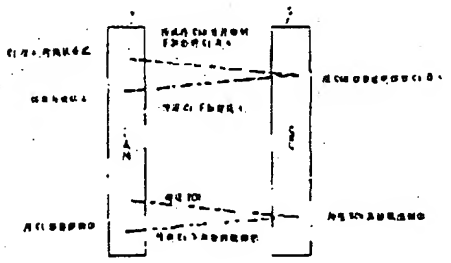
[74]专利代理机构 中国国际贸易促进委员会专利商标事务所
代理人 杨国旭

权利要求书2页 说明书3页 附图页数2页

[54]发明名称 在两个设备之间提供安全通信的方法及该方法的应用

[57]摘要

在两个设备之间提供安全通信的方法中，第一设备生成随机密钥(C_i)并在采用公开密钥加密的第一报文中将这一密钥传送给第二设备。第二设备用对应的秘密密钥解密第一加密报文以获取该随机密钥(C_i)并用这一随机密钥来加密与解密这两个设备之间的所有传输。在收费电视系统的解码器中，包含条件接入模块及智能卡，应用这一方法来提供控制接入模块与智能卡之间与/或解码器与条件接入模块之间的安全通信。



ISSN1008-4274

专利文献出版社出版

权 利 要 求 书

1.在两个设备之间提供安全通信的方法，其中，第一设备生成随机密钥(C_i)并在用公开密钥加密的第一报文中将所述密钥传送给第二设备，其中所述第二设备用对应的秘密密钥解密第一加密报文以获取所述随机密钥(C_i)，其中利用所述随机密钥来加密与解密所述设备之间的传输。

2.按照权利要求1的方法，其中解密了所述加密的报文之后，所述第二设备首先在带有鉴别的第二加密报文中返回所述随机密钥(C_i)给所述第一设备。

3.按照权利要求2的方法，其中为了提供所述鉴别，所述第一设备还生成随机数（A）并在所述第一加密报文中将这一随机数（A）与所述随机密钥（C_i）一起传送给第二设备，其中该第二设备利用所述随机数（A）供在第二加密报文中鉴别。

4.按照权利要求3的方法，其中所述第二设备在所述随机密钥(C_i)下加密所述随机数（A）来获得所述第二加密报文。

5.前面的权利要求中任何一项中的方法在收费电视系统的解码器中的应用，其中所述解码器包括条件接入模块（CAM）及智能卡（SC），其中应用所述方法来提供控制接入模块与智能卡之间的安全通信。

6.权利要求1－4中任何一项中的方法在收费电视系统的解码器中的应用，其中所述解码器包括条件接入模块（CAM）及智能卡（SC），其中应用所述方法来提供解码器与条件接入模块之间的安全通信。

7.收费电视系统的解码器，包括条件接入模块及智能卡，所述条件接入模块包括用于生成随机密钥(C_i)的装置、利用公开密钥加密方法在第一加密报文中加密所述密钥的装置、传送所述第一加密报文到智能卡的装置，所述智能卡包括用于接收与解密所述第一加密报文以获得所述随机密钥的装置、用于在所述随机密钥下加密对

条件接入模块的传输的装置，所述条件接入模块具有解密从智能卡接收的所述传输的装置。

8.按照权利要求7的解码器，其中所述智能卡包括用于在带有鉴别的第二加密报文中将所述随机密钥返回给条件接入模块的装置。

9.按照权利要求8的解码器，其中条件接入模块的所述生成装置还生成包含在所述第一加密报文中的随机数，其中该智能卡适应于采用所述随机数作为第二加密报文中的鉴别。

10.收费电视系统的解码器，包括条件接入模块及智能卡，其中所述解码器包括用于生成随机密钥（ Ci）的装置、用于采用公开密钥加密方法在第一加密报文中加密所述密钥的装置、用于传送所述第一加密报文到条件接入模块的装置，所述条件接入模块包括用于接收与解密所述第一加密报文以获取所述随机密钥的装置、用于在所述随机密钥下加密对解码器的传输的装置，所述解码器具有解密从条件接入模块接收的所述传输的装置.

11.按照权利要求10的解码器，其中所述条件接入模块包括用于在带有鉴别的第二加密报文中返回所述随机密钥给解码器的装置。

12.按照权利要求11的解码器，其中解码器的所述生成装置还生成包含在所述第一加密报文中的随机数，其中该条件接入模块适应于利用所述随机数作为第二加密报文中的鉴别.

说　　明　　书

在两个设备之间提供安全通信的方法及该方法的应用

本发明涉及在两个设备之间，特别是在收费电视系统中所使用的设备之间，提供安全通信的方法。

在收费电视系统中，各用户通常具有用于破密源分量信号的解码器，其中所述解码器包括用于解密权利控制报文及权利管理报文的条件接入模块及智能卡。为了防止将解码器的未授权操作用于破密源分量信号，例如防止在授权与未授权的智能卡之间转换是重要的。

本发明旨在提供上述类型的方法，其中以这样的方式来配置诸如控制接入模块与智能卡或解码器与条件接入模块这两个设备之间的通信，使得授权与未授权的设备之间的转换是不可能的。

按照本发明，提供了一种方法，其中第一设备生成随机密钥（ C_i ）并在用公开密钥加密的第一报文中将所述密钥传送给第二设备，其中所述第二设备利用对应的秘密密钥解密该第一加密报文来获得所述随机密钥（ C_i ），其中所述随机密钥用于加密与解密所述设备之间的进一步传输。

按照本发明，这一方法能应用在收费电视系统的解码器中，其中所述解码器包括条件接入模块及智能卡，其中应用所述方法来提供控制接入模块与智能卡之间或解码器与条件接入模块之间的安全通信。

本发明进一步提供用于收费电视系统的解码器，包括条件接入模块及智能卡，所述条件接入模块包括用于生成随机密钥（ C_i ）的装置、用于在使用公开密钥加密方法的第一加密报文中加密所述密钥的装置、用于将所述第一加密报文传送到智能卡的装置，所述智能卡包括用于接收与解密所述第一加密报文来获得所述随机密钥的装置、用于在所述随机密钥下加密对条件接入模块的传输的装置，所述条件接入模块具有解密来自该智能卡所接收的所述传输的装置。

在本发明的又一实施例中，所述解码器包括条件接入模块及智能卡，其中所述解码器包括用于生成随机密钥（ C_1 ）的装置、用于在使用公开密钥加密方法的第一加密报文中加密所述密钥的装置、用于将所述第一加密报文传送到该条件接入模块的装置，所述条件接入模块包括用于接收及解密所述第一加密报文来获得所述随机密钥的装置、用于在所述随机密钥下加密对解码器的传输的装置，所述解码器具有解码从条件接入模块接收的所述传输的装置。

通过参照在其中说明应用在收费电视系统中的本发明的方法的实施例的附图，进一步说明本发明。

图 1 示出按照本发明的解码器的实施例的方框图。

图 2 示出本发明的方法的实施例的步骤序列.

参见图 1，其中以非常示意性的方式示出了用于收费电视系统的解码器的方框图，其中按照诸如 Eurocrypt 标准用控制字扰频数字信息信号。在本实施例中，解码器包括解调器 1、信号分离器 2 及解压单元 3。解码器还包括条件接入模块或 CAM 4 及智能卡 5，后者能插入条件接入模块 4 的连接槽中。此外解码器还设置有用于配置与控制目的的微处理器 6.

条件接入模块 4 设置有破密器单元 7 及具有存储器 9 的微处理器 8。智能卡 5 包括具有存储器 11 的微处理器 10.

由于解码器的上述部件的操作不是本发明的一部分，将不详细描述这一操作。通常，解调器 1 所接收的信号为在 950 MH_z 与 2050 MH_z 之间的经过调制的数据流。解调器 1 的输出为提供给 CAM 4 的加密数字数据流，而假定已插入了授权的智能卡且用户有权接收节目，便允许破密器 7 破密这一加密数据流。信号分离器 2 分离破密后的数据流信号并由解压单元 3 将其解压及转换成原来的模拟音频与视频信号.

在收费电视系统中，破密所需的控制字是在用服务密钥加密的包含该控制字的所谓授权控制报文中传送给用户的。这一服务密钥是用诸如称作授权管理报文下载到智能卡 5 的存储器 11 中的.操作期间，CAM 4 将授权控制报文传送到智能卡 5 的微处理器 10，使得微处理器 10 能处理该授权控制报文并抽取控制字。此后，智能卡 5 将解密的控制字返回

到 CAM 4，从而允许破密器 7 破密从解调器 1 接收的数字数据流。

为了防止结合 CAM 4 使用未授权的智能卡 5，提供 CAM 4 与智能卡 5 之间的安全通信是重要的。按照本发明，采用了下述方法来提供这一安全通信。图 2 中示出这一方法的步骤。当将智能卡插入解码器中时，CAM 4 的微处理器 8 生成两个随机数 C_i 与 A。微处理器 8 在 CAM 4 的公开密钥下在第一报文中加密随机数 C_i 与 A。将这样得出的第一报文传送给智能卡 5 而微处理器 10 用 CAM 4 的秘密密钥解密这一第一报文。此后微处理器 10 返回第二报文给 CAM 4，所述第二报文为在用作密钥的数 C_i 下加密的随机数 A。CAM 4 的微处理器 8 解密这一第二报文并检验随机数 A 是否正确。假定随机数 A 是正确的，因此可以认为插入的智能卡 5 是授权的智能卡，这时 CAM 4 将包含加密的控制字的授权控制制报文提交给智能卡 5，后者以传统方式处理该授权控制报文并抽取该控制字。然而，在对 CAM 4 的返回报文中，智能卡将提交在密钥 C_i 下加密的所抽取的控制字，而这些加密的控制字则由微处理器 8 用相同的密钥 C_i 解密。一旦有人试图用其它智能卡替代插入的智能卡 5，例如通过从授权的智能卡 5 转换到非授权的智能卡，由于新的智能卡不知道密钥 C_i 而 CAM 4 立即觉察这一改变，从而 CAM 不再能破密包含控制字的返回报文。从而使破密单元 7 不能工作。

能以相同的方式利用上述方法来提供 CAM 4 与解码器之间的安全通信，其中遵守图 2 中所示的相同协议。

简言之，可以理解如果将新的 CAM 4 连接到其它解码器部件上，解码器的微处理器 6 将生成这两个随机数 C_i 与 A，并且在微处理器 6 解密了从 CAM 4 的微处理器 8 所接收的第二报文并检验出随机数 A 为正确的时，便立即在 CAM 4 与微处理器 6 之间的所有传输中使用密钥 C_i。

本发明不限于上述实施例而能在权利要求书的范围内以多种方式变化。作为另一实施例的示例，该 CAM（即破密器）可以是解码器的一部分。解码器这时会查问智能卡来证明它自己以获得智能卡与解码器之间的安全通信。

说 明 书 附 图

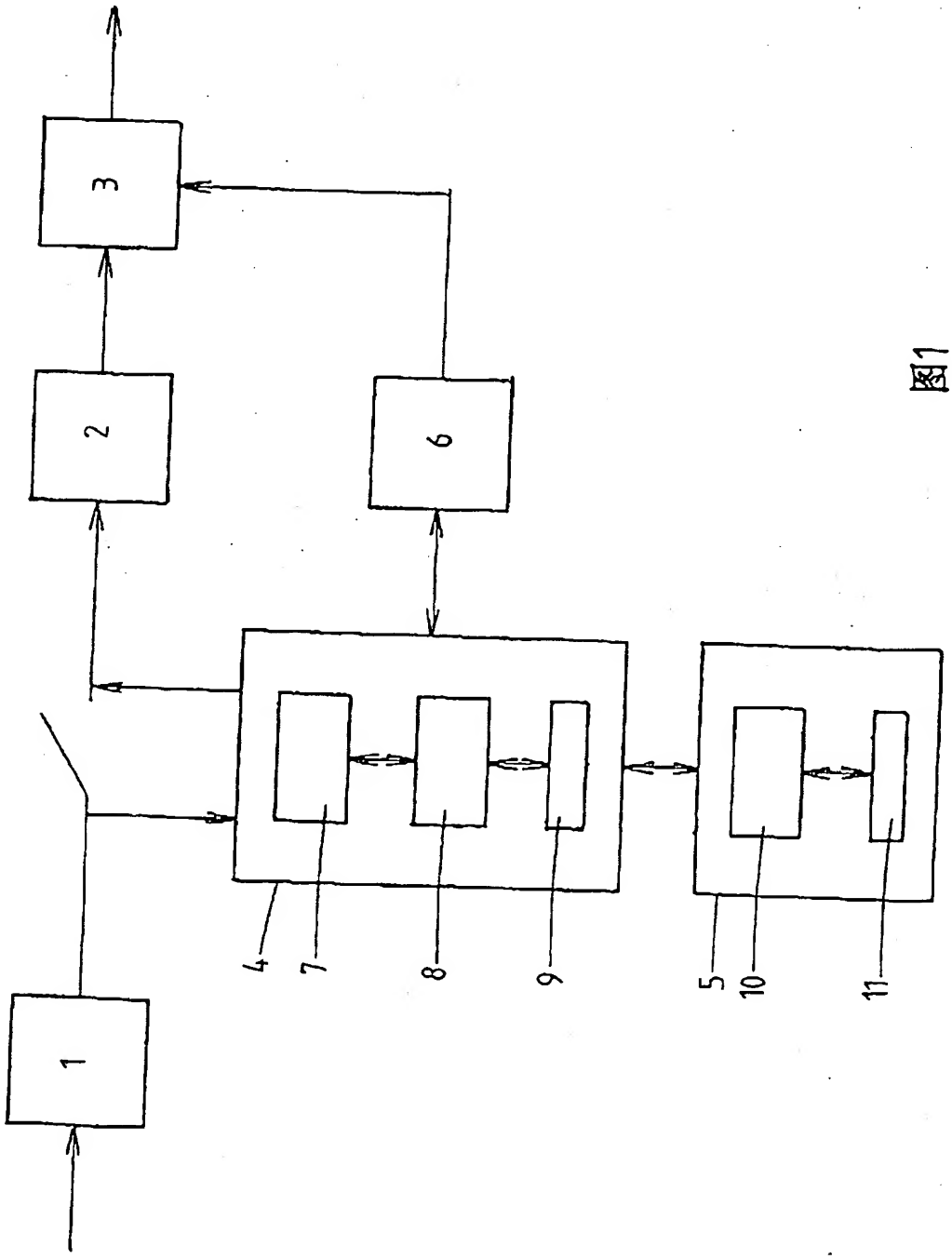


图1

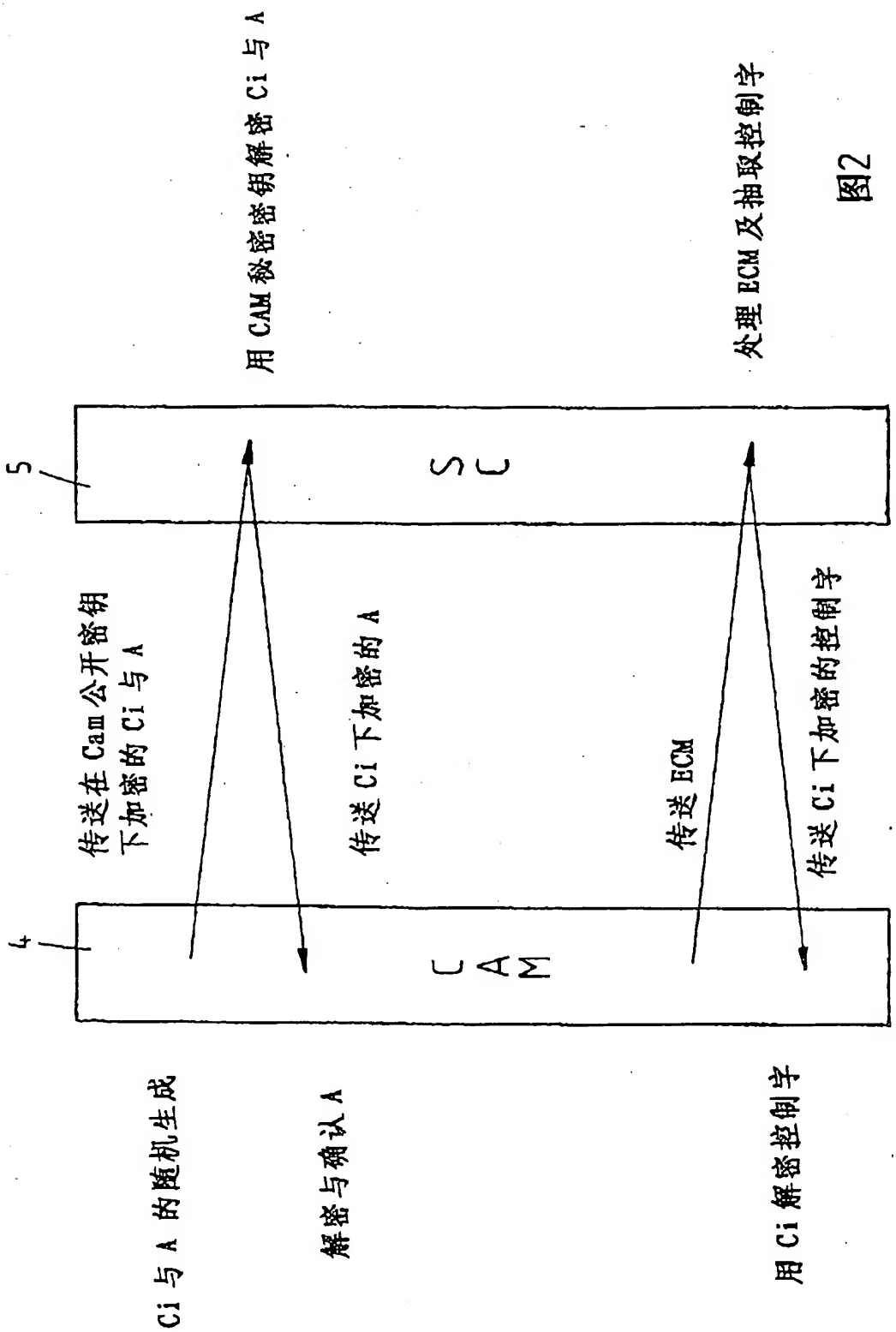

5
4
SC
CAM
用 CAM 秘密密钥解密 Ci 与 A
处理 ECM 及抽取控制字
传送在 Cam 公开密钥
下加密的 Ci 与 A
传送 Ci 下加密的 A
传送 ECM
传送 Ci 下加密的控制字
Ci 与 A 的随机生成
解密与确认 A
用 Ci 解密控制字

图2

网络工程

电子商务中的安全机制探讨

中国科技大学电子工程与信息科学系(合肥 230027) 林凌峰 徐守时 蒋智宁

摘 要 安全性是电子商务进一步发展的一大障碍,文章简要介绍了现代密码学的发展及其在电子商务中的应用,分析了电子商务中的安全机制,并以 SET 协议为例给出了一个加密解密流程。

关键词 电子商务 密钥加密 Hash 算法 SET 数字签名 数字信封 证书

随着电子商务的兴起,Internet 也正式进入了商业活动领域,预计到 2003 年,网上的电子交易额将超过 1 万亿美元。但是由于 Internet 在结构上缺乏对信息的保密措施,如何安全地在 Internet 上开展商务活动,一直是研究的一个热点。现在也有包括 EDI (electronic data interchange)、SSL (secure sockets layer)、SET (secure electronic transaction)、SEP(安全电子付款)等多种基于 Internet 安全传送的标准和解决方案。这些协议主要都是利用现代密码学的技术,来构筑 Internet 上的安全体系。

1 现代密码学技术

现代密码技术从 1949 年 Shannon 发表的著名论文"Communication Theory of Secrecy System"以来,经过几十年的长足发展,现正应用于并行超大规模计算机的加密和解密,成为计算机网络和安全通信中的一门关键技术。现在流行的主要有以下两种加密机制。

1.1 对称密钥加密体制

所谓对称密钥加密机制是指加密和解密过程所用的密钥相同,著名的有 DES、IDEA 等算法。DES (Data Encryption Standard)是第一个公开的加密体制,1975 年由 IBM 研制发表,1977 年美国将其定为非绝密文件的加密规范,是现在民用加密中的常见标准。

DES 的密钥长度为 64bit (实际有效长度为 56bit,另外 8bit 是奇偶校验位),加密时将输入信息分为 64bit 一组进行操作,通过一个初始变换,打乱明文,然后分左右各 32bit 进行 16 次迭代运算,最后再进行一次左右 32bit 交换和反初始交换。与此同时,56bit 的密钥作循环转置和缩减转置,产生 16 组 48bit 的子密钥,供加密时的 16 次迭代使用。其一次处理过程如图 1 所示,其中加密函数 f 的功能是 DES 算法的关键。解密操作和加密操作基本相同,只是第一次迭代前要先将 32bit 左右互换,每个密文块经过 16 次迭代得到明文块。

但是,20 世纪 90 年代后,有人提出"差分分析法"、"线性逼近法"等攻击方法,同时随着集成电路和高性能计算机的飞速发展,采用全部逐一搜索密钥的方法来攻击 DES 算法也渐渐成为可能。由此也提出了一些 DES 算法的变形,如增加密文和密钥的长度、增加迭代次数、结构上引入反馈方式、改变 S_i 等等。此外,DES 算法的思想已为很多分组加密算法所继承,包括较流行的算法 IDEA (International

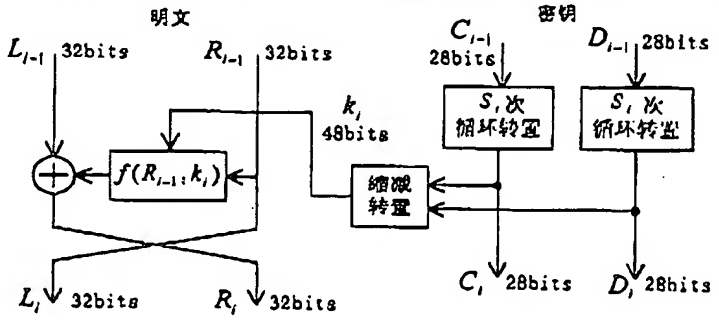


图 1 DES 的一次迭代过程

Data Encryption Algorithm,即国际数据加密算法,由瑞士科学家提出)。IDEA 基本上模仿 DES 的结构,密钥长度为 128bit,较 DES 更安全。

在对称密钥加密机制中,系统的保密性由密钥的保密性决定,如何管理密钥和让接收方安全获得密钥是一个困难的问题,而且当一个用户要和其他很多用户进行通信时,这样多的密钥管理也是一个难题。因此又提出了公开密钥加密体制。

1.2 公开密钥加密体制

1976 年斯坦福大学的 Diffie 和 Hellman 在论文"New Direction in Cryptography"中提出了公开密钥加密体制,简要地说,即系统的加密密钥和解密密钥不同,而且解密密钥很难由加密密钥推出。这之后提出有 RSA(1978 年,取三位发明者 Rivest,Shamir,Adleman 的首字母)、背包算法(1978 年,Merkle 和 Hellman)、椭圆曲线算法(1993 年,Menezes 和 Vanstone)等不少公钥加密算法出现。RSA 算法的安全性是建立在大数分解的困难性上面,此后还出现了 RSA 算法的 Robin 修正,可看成是 RSA 的一个特例。最初的 MH 背包算法曾被 Shamir 攻破过,通常只作理论研究,后来也出现了其他形式的背包算法。椭圆曲线算法利用椭圆曲线上有理点的异或运算,构造椭圆曲线上的有限域,也是一种很有前途的加密算法。

这里介绍一个用得比较多的 RSA 算法。

RSA 算法基于数论原理,其步骤如下:

(1) 选择两个质数 p 和 q,p、q 均大于 10^{100};

(2) 计算 $n = p \times q$ 和 $z = (p-1) \times (q-1)$;

(3) 选择一个和 z 互质的数 e;

(4) 找出 d,使得 $e \times d = 1 \pmod z$。

这样 (e, n) 作为公开密钥予以公布,而 (d, n) 为私人密钥。加密时将明文分块数字化,每个分块的长度小于 $\log_2(n)$,其对应数字设为 m,则加密算法为:$C = E(m) = m^e \pmod n$;解密算法为:$D(C) = C^d \pmod n \equiv m$。

解密的正确性可由数论中的欧拉定理推出,可参见文献[1]或应用数学方面的书刊。这样和甲用户通信的其他用户都可以用甲用户的公开密钥加密信息,再传送出去,而只有用甲的私人密钥才可以进行解密。

在这两种加密体制中,通常对称密钥的加密解密效率比较高,一般比公开密钥加密快 10 倍以上,但是缺点是若密钥没有安全的方式传送,易被截获,且如果和大量用户通信,难以安全管理这么多密钥,不太适宜大范围应用。而公钥加密的优缺点则相反,故公钥加密常用于少量数据的加密,如在电子商务中,可以用于对称密钥的传送。

2 电子商务中的安全机制基础

在电子商务中,其安全机制至少要保证信息的保密性和完整性,并具有身份鉴别和反拒认功能。其中信息的完整性指的是保证信息未遭破坏或非法篡改,反拒认指的是在敏感的交易过程中,防止对方拒绝承认他已经发送的信息或已要求的事物处理。

目前已有不少电子商务安全方面的协议,我们以 SET 为例来说明电子商务中的安全机制。SET 协议综合使用了包括对称密钥加密、公开密钥加密、Hash 算法、ASN.1、X.509、PKCS 等现有的加密技术和标准,并产生了数字签名、数字信封、数字证书等概念(数字证书的概念十分重要),而且对各种报文信息的保密性、完整性和不要否认性作了详细的划分,将密钥数目和加密操作减少到最小程度,它的很多思想都可以作为安全系统设计的借鉴。

2.1 对称密钥加密和公开密钥加密

如前面所述的对称密钥加密机制和公开密钥加密机制的优缺点(用软件实现 DES 算法比 RSA 快约 2 个数量级,用硬件实现的话,大约快 3 个数量级),在 SET 协议中用对称密钥加密(缺省用 DES)进行明文的加密,密码可以随机选取,再用公开密钥加密法(缺省用 RSA)进行对称加密密钥的传送。

2.2 Hash 算法

对任意长度的信息,经过 Hash 函数运算后,都可压缩成固定长度的数字,而且这数字对源信息有高度的敏感性。SET 协议中用 SHA-1(Secure Hash Algorithm)安全 Hash 算法,来产生数字签名。它可以处理任意大小的信息,生成 160bit 的信息摘要,信息的微小变化都会在信息摘要上产生明显的变化,而且就算已知信息摘要,也极难推断出源信息。

此外,为防止重发攻击(play back),在 SET 协议里还使用了随机数标志。所谓重发攻击就是将发送方的信息全部截获下来,再按照顺序发给接收方。SET 协议里请求方发送的请求信息里包含了随机数,接收方在响应报文的特定位置填入该随机数,再一起加密发送,这样请求方如果在一定时间内收到同一发送方发出的同一随机数标志(或时戳)的信息,就可以认为是重发攻击而不予理睬或采取其他安全措施。

2.3 SET 协议中完整的加密解密过程

这里给出 SET 协议中加密解密的一个完整的

流程。加密过程如图 2 所示,解密过程如图 3 所示,下面解释一下数字签名、数字信封和数字证书。

3.1 数字签名

要发送的明文通过 Hash 算法形成信息摘要,再用发送者(甲方)的私人密钥进行加密,生成的就是数字签名,将其附在原信息上发送;而接收者(乙方)收到数字签名后,用甲方的公开密钥进行信息摘要的解密,同时将收到的明文再通过 Hash 算法得到信息摘要,比较这两者(即图 3 中的信息摘要 1 和信息摘要 2)。若一致,则表示该信息是完整的,没被破坏或非法改动,也说明收到的信息确实来自甲方(因为证书中的公开密钥和发送者的私人密钥是成对的,甲方的公开密钥包含在数字证书中,乙方还可以通过认证证书的有效性,来证实甲方的身份)。另外,若甲方拒认,数字签名还有反拒认功能。

3.2 数字信封

甲方将其对称密钥用乙方的公开密钥进行加密,形成数字信封,发送出去。乙方收到后,用自己的私人密钥解密,获得甲方对称加密所用的密钥,来解开密文信息。

3.3 数字证书

数字证书是 SET 协议里最具特色的部分,主要用以确认发送方的公开密钥的有效性,是由一个双方都信任的第三方权威机构 CA(certificate authority)发布的。数字证书中包含了所有者的公开密钥、个人资料的摘要和证书签发机构的数字签名。现行的证书标准如 X.509、ASN.1(Abstract Syntax Notation 1)是 ISO 制订的描述抽象对象的语法表示方法。SET 协议的数字证书管理部分[3,4,5]十分完善,SET 的证书管理模型为其他安全系统的设计提供了完整的参考模型。

4 电子商务的现状和未来

电子商务的发展有两个重要的障碍,一个是 Internet 上传送的安全性,另一个是现有几种协议的互通和标准化,以及对原有协议和网络的继承性。现在的几种技术各有优缺点。SET、SSL、EDI、SEP 都在一定程度上提供了电子商务活动的安全性。其中,SSL 协议主要只是一种面对网络的安全技术,缺乏证书管理措施,身份识别功能较弱;SET 协议主要针对银行信用卡业务;EDI 是 20 年前就出现的电子交换数据标准,不是特别适合 Internet 上的用户和贸易商直接进行交易,而且显得过于庞大,修改过于烦琐。

SET 协议的证书管理体系很有特色,必将得到越来越广泛的应用。但是 SET 协议在流程方面也存在一些缺陷,诸如贸易商如何来完全确信一张有客户认证的帐单?银行怎么核准用户收到的证书?而且,SET 协议给实际操作很大的自由度,如允许银行在完成交易后将客户的信用卡号码传给贸易商,这样也造成了一种潜在的威胁。预计近期推出的 SET 2.0 版中会有改进。现在出现的智能卡技术将对 SET 协议进行有力的挑战。

在现实的系统中使用分级授权、密钥管理、加密

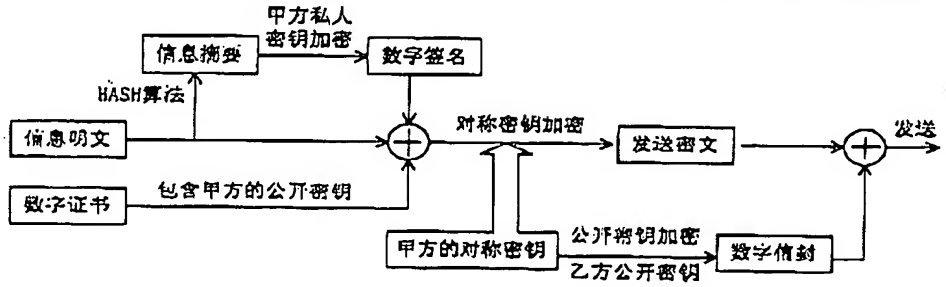


图 2 SET 协议中的加密流程

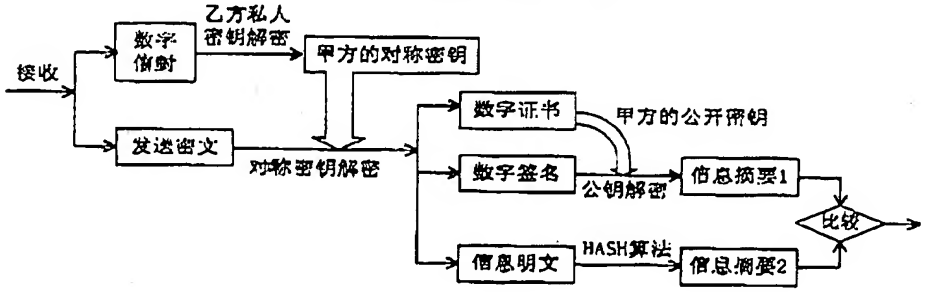


图 3 SET 协议中的解密流程

网络工程

一种宽带接入网的设计方案

上海交通大学自动化系(上海 200030) 高 峰 谢剑英
上海电信设备一厂(上海 201801) 滕正利 张 蔚

摘 要 文章介绍了一种光纤到大楼加上多媒体引入线的宽带接入网的设计方案,并从接入技术、组网结构、系统配置等方面作了详细的介绍。最后给出了详细的设计方案图。

关键词 宽带接入网 多媒体引入线 SDH

1 概述

接入网(AN)泛指用户网络接口(UNI)与业务节点接口(SNI)间实现传送承载功能的网络实体,其目标是建立一种标准化的接口方式,使用户能够获得话音、租用线业务、数据多媒体、有线电视等综合业务。由于传统的电信网主要是电话业务,接入网部分就是简单的用户线。随着电信业务的不断发展,接入业务已由简单的话音信号转向数据、图像等多种业务,接入频带由音频转向视频,这样,接入网部分就必须由简单的用户线转向宽带接入网。

国内接入网的发展可分为以下几个阶段:(1)启动阶段(1996～1998 年),业务以 POTS、数据和 TV 为主,在城市里以解决金融部门的通信需求为契机,开始部分实现光纤到大楼(FTTB);(2)发展阶段(1999～2002 年),N-ISDN 业务开始增长,光纤到大楼(FTTC)和 FTTB 在网络中占的比例较大;(3)普及阶段(2002～2005 年),主要有 POTS、高速数据、CATV、宽带多媒体等业务,将大量采用 FTTC 和 FTTB,商用光纤到家庭(FTTH)开始出现。上海从 1996 年底开始,在上海邮电管理局的领导下,统一规划、统一建设,加快了实现 FTTB 和 FTTC 的步伐。1999 年,上海邮电又以某小区为试点,在新建小区内实现宽带接入方式。

2 宽带接入网技术

接入网的接入方式主要分为有线接入和无线接入两种。在有线接入方式中,目前有铜缆接入、光纤接入和光纤同轴混合接入(HFC)等技术。

铜缆接入新技术包括铜线数字化技术,线对增容(pair gain)技术、高比特率数字用户线技术(HDSL)、不对称数字用户线技术(ADSL)等。它可以增强铜缆接入的灵活性和业务承载能力,使其能在短时间内提供用户线对增容,并能够传送 ISDN 等数字业务。例如,ADSL 接入技术主要承载的业务有 POTS、租用线业务以及 VOD 等,它在 1 对上下行信道传输能力不对称的电话线上既可传输语音信号又可同时传输视频信号,其带宽一般为 6～8Mbit/s。应用铜缆接入新技术可有效地利用现有的铜线基础设施,但传输速率较低,传输距离有限(3～5km),难以适应各种接入设备传输距离的要求及宽带业务发展的需要。因此,这几种接入技术适合作为建设光纤接入网期间的过渡措施或作光纤接入网的补充。

传输、会员管理以及 IC 卡网上认证等办法,使信息的安全性得到更切实的保证。在未来的几年里,电子商务将有长足的发展,未来的电子商务将是内容丰富的、方便的、保密的、安全的和易于扩展的。这里的安全性不仅仅是技术上的问题,还包含用户对系统开发商、认证机构的信心,以及对非面对面交易的信赖程度。

参 考 文 献

1 卢开澄. 计算机密码学 ——计算机网络中的数据保密和安全. 北京:清华大学出版社,1998
2 Secure Electronic Transaction Specification Book 1: Business Description, Version 1.0. 1997,5
3 Secure Electronic Transaction Specification Book 2: Programmer's Guide, Version 1.0. 1997,5
4 Secure Electronic Transaction Specification Book 3: Formal Protocol Definitions, Version 1.0. 1997,5
5 IBM. Secure Electronic Transaction: Credit Card Payment on the Web in Theory and Practice. International Technical Support Organization, 1997,6